Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE DIVISION OF INFORMATION RESOURCES MANAGEMENT'S CHANGE CONTROL PROCESS

OFFICE OF INSPECTOR GENERAL

(A9505) **February 1996**

TABLE OF CONTENTS

Page

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL
February 1996

Mr. S. David Frost, Chairman
Automation Policy and Programs Committee

Mr. Stephen R. Malphrus, Director
Division of Information Resources Management

We are pleased to present our final *Report on the Audit of the Division of Information Resources Management's (IRM's) Change Control Process* (A9505). We performed this audit to review the efficiency and effectiveness of IRM's change control process and to assess IRM's role and responsibilities for coordinating and developing change control guidelines for distributed systems.

Overall, we found that IRM has taken steps to implement new change control procedures and is committed to controlling changes to the Board of Governors of the Federal Reserve System's (the Board's) information technology environment. IRM has not, however, integrated these procedures into a comprehensive change control process and the procedures are not being consistently implemented. Furthermore, we found that security over application software does not properly reflect the roles, responsibilities, and separation of duties normally present in an effective change control process. Given the Board's significant investment in information technology and the degree of change that is occurring, we believe that IRM needs to develop a more comprehensive change control process and improve security over its mainframe-based application software.

We also found that no one has assumed responsibility at the Board for advocating, developing, and disseminating change control guidelines for distributed systems. We believe that the Board's Automation Policy and Programs Committee (APPC) should provide leadership in this area.

We provided a draft of this report to you for review and comment. The Director of IRM’s response, which we understand was discussed with the chairman of the APPC, has been included as appendix 1. The director generally disagrees with our recommendations, but indicates that some steps will be taken to strengthen the existing change control procedures and restrict programmer access. Not withstanding these actions, we continue to believe that the Board should more closely follow standard industry change control practices. Implementing the recommendations in this report would go a long way in achieving this purpose.

As always, we will be happy to respond to any questions that you may have. We are sending copies of this report to the Administrative Governor and heads of the Board's offices and divisions. It will also be summarized in our next semiannual report to the Congress. We will follow up on the actions taken with respect to our recommendations at a later date.

Sincerely,

Barry R. Snyder
Assistant Inspector General for Audits

BACKGROUND

The Board maintains a substantial inventory of computer hardware, system software, and application software (both in-house-developed and commercial off-the-shelf) to achieve its strategic automation and information objectives. Board employees use this inventory of information technology to collect and process large volumes of data submitted by the Federal Reserve Banks, commercial banking institutions, and other governments agencies. Members of the Board and Board staff use the data as input to monetary policy, bank supervision, and payment system decisions.

The Board has a substantial investment in its information technology. According to Board budget and performance reports covering the period 1992 through 1994, an estimated $91.3 million was expended for mainframe and distributed computing resources (See table 1 below). These ongoing investments in information technology indicate that the Board's information processing systems are in a continuous state of change as technological innovations are introduced and as organizations seek new ways to use information systems to become more efficient and effective.

Table 1
Division of Information Resources Management (IRM) and Distributed Processing Expenses 1992-1994[1]

	IRM Expenses*	Estimated Distributed Processing Expenses	Total Expenses
1992	$ 22.2 M	$ 6.3 M	$ 28.5 M
1993	$ 23.6 M	$ 7.2 M	$ 30.8 M
1994	$ 23.6 M	$ 8.4 M	$ 32.0 M
Total	$ 69.4 M	$ 21.9 M	$ 91.3 M

*IRM expenses include data management services performed by Statistical Services, Statistical Reports Support, NIC Operations, and HMDA Operations and management services performed by Special Services.

Given the level of investment and the degree of change, it is important that the Board have an effective change control process. Such a process should be designed to protect the organization's significant investment of money, time, and effort to acquire and maintain its

Information presented in table 1 was extracted from the 1992, 1993 and 1994 Performance Reports published by the Office of the Controller. IRM expenses represent the operating total of actual expenses in the IRM Financial Performance by Program and Object of Expenditure. Distributed processing expenses represent estimated funds expended for distributed processing systems and resources that are generally controlled by the individual divisions and reside on local area networks, workstations, and microcomputers. Specific costs associated with distributed processing have not historically been segregated or tracked, but they were estimated in the 1994 Performance Report.

computer hardware and system software and to buy or develop its application software. Changes to information technology create vulnerabilities. If information technology is inadequately protected, computer programs could be inadvertently changed or deleted or critical data inadvertently modified. Another possible vulnerability is manipulation of software for personal gain. Information technology is also vulnerable to more subtle threats such as those posed by disgruntled employees. Employees who have access to information technology can cause significant damage by altering or damaging hardware and software. The damage may not be detected until long after the employee has left and could have significant adverse impact if operations are disrupted or assets destroyed.

Elements of an Effective Change Control Process

An effective change control process generally consists of a set of procedures and safeguards designed to ensure that changes to an organization's information technology do not disrupt business operations and that an organization's investment in information technology is adequately safeguarded. The process normally consists of a series of management reviews and approvals that ensure that only authorized and intended changes are made. Usually, the user prepares a change request form describing the desired change to enhance system functions or to meet changing business requirements. Information technology managers review the request and assign a programmer/analyst to analyze the impact of the requested changes and determine the specific hardware and/or software that will need to be changed to satisfy the request.

An approved change to in-house-developed application software normally involves the copying of the current production version of the application software into a development workspace. The assigned programmer/analyst modifies the copy of the software in the developmental workspace and follows a plan to test the modifications. After initial testing by the programmer/analyst, the development copy is moved to a test workspace and the user is asked to independently test and validate that the requested changes have been made and business requirements have been satisfied. Upon certification by the user that the changes operate as intended, the new version of the application software is installed to the production environment. Once placed in the production environment, the software is placed in a restricted and controlled software library management system from which it can be processed by the appropriate computer systems.

Effective change control procedures are also required to plan, control, distribute, and install modifications to hardware, system software, and communications network systems. Similar to applications software change control, these procedures include recording requests, reviewing the requests and assigning one or more specialists, determining the specific hardware and/or software that will need to be modified, making the changes, testing all the modifications and verifying that the requested changes meet business requirements, and placing the specific hardware and/or software into production.

The Board continues to migrate many of its automated applications to distributed systems. These systems have similar levels of risk, but the controls are less structured than those normally found in mainframe systems. These systems also need to have well documented and implemented change control procedures to ensure that all elements have been tested and proven to work together.

IRM's Change Control Process

To manage its hardware, system software, communication network systems, and application software modifications, and ensure their integrity, IRM developed and implemented new change control procedures during 1994. The procedures consists of a change control form and instructions on how to fill it out. The form contains background and control information such as change number, manager and IRM lead assignments, and project name. Additionally, the form logs approvals for the initiation, development, quality assurance, and production implementation of software changes. IRM also uses several automated library systems to control its software.

OBJECTIVES, SCOPE, AND METHODOLOGY

We performed an audit of IRM's change control process from March 1995 to September 1995. Our audit objectives were to evaluate the effectiveness of IRM's change control process and to assess IRM's role and responsibilities for coordinating and facilitating change control awareness and developing and disseminating change control guidelines to distributed processing groups. To accomplish our objectives, we reviewed policies, procedures, and related change control documentation; interviewed Board officials and staff; and tested security over production software libraries and compliance with the accuracy and verification controls identified in IRM's change control process. We judgmentally selected five of eight IRM sections where the new change control procedures had been implemented to test for compliance with the new procedures. We interviewed officials and staff from IRM and four Board divisions and offices about the need for a Boardwide change control process and IRM's potential role in sponsoring the development of change control procedures for distributed systems. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

IRM has taken steps toward implementing a change control process for the Board's mainframe environment. It organized a committee to address the need for change control procedures, developed a change control form that could be used for both hardware and software changes, and held a meeting to communicate the new procedures. Even though these actions reflect a commitment by IRM to control changes to the Board's information technology, we believe that these steps do not provide an adequate level of change control over the Board's material investment in automation assets. Specifically, we found that (1) change control procedures are described in several different documents making them difficult to understand and follow, (2) compliance with the procedures varies from section to section, and some sections continue to use procedures developed specifically for their section, and (3) access to application software is not adequately restricted to reflect the roles, responsibilities, and separation of duties inherent in an effective change control methodology. We also found that no one has assumed responsibility at the Board for advocating, developing, and disseminating change control guidelines for the Board's distributed processing environment.

The following recommendations are designed to enhance the Board's change control process for both its mainframe and distributed processing environments.

1. We recommend that the Director of IRM develop an integrated, comprehensive change control process and ensure that all IRM sections implement it.

Based on the interviews and tests we conducted, we found that IRM's new change control procedures and related form are not being used consistently by all IRM sections. We determined that ten of the fourteen IRM sections interviewed used the recently developed change control form. For those sections tested that use the form, we found forms that were only partially completed with inconsistent data being recorded from section to section. Other sections have supplemented the new form with additional documents to provide detailed work-order type descriptions of changes and associated operational activities. In several sections where the form was not used, we were told that different forms and automated systems were being used to document and manage changes.

Our tests indicate that the current instructions lack sufficient detail to convey to IRM staff and users how the procedures are to be applied and in what context. We believe that IRM needs to incorporate the current change control form and instructions into a more comprehensive change control process that identifies and describes the major activities that the Board relies upon to control and manage changes to its information technology and the associated roles and responsibilities of IRM staff and users in the process. We believe that a more comprehensive process, when implemented,
would provide several positive benefits. Specifically, roles and responsibilities will be clarified; an audit trail will exist to track changes and to help understand the cause of any problems in the event that they occur; and users will have consistent, unified access to information regarding changes.

2. We recommend that the Director of IRM implement a consistent approach to software library management including a more restrictive approach for programmer/analyst access to application software.

IRM uses several different software library management systems and its approach to using them varies from section to section. Software is currently stored in two library management systems: Panvalet and Endevor. Some sections uniformly store all software in a single library management system; other sections split the storage of different categories of software between a library management system and operating system files. We believe that use of multiple products is inefficient because it necessitates different procedures for each product, increases the learning curve for new employees, and creates a potential for increased costs associated with maintaining multiple library management systems. Therefore, we believe that IRM should select a single library management system and implement consistent procedures for its use.

We also found that IRM does not consistently restrict access to software within and across library management products. Programmers, including both Board employees and contractors, can access and update application software that they are not authorized to modify. They can access all software within their own section and software that is developed and maintained by other sections, instead of just the software they have been assigned to maintain. As a result, software could be inadvertently or intentionally altered and the changes could lead to the disruption of Board operations or other problems including reduced data integrity. We believe the Board's significant investment in its computer software and data requires a more restrictive approach to software access to reduce the Board's risk of loss.

3. We recommend that the Director of IRM establish policies and procedures restricting programmer access to production data to an emergency-only basis.

We found that Board programmers in IRM sections have been given a range of access to production data in Board application software systems. Some sections' programmers can directly access and update production data. One other section restricts programmer access to a single programmer; another section does not allow programmer access to production data at all.

We believe a data security policy should be established restricting programmer access from production data except in cases of emergencies when quick resumption of processing is required. This restriction decreases the risk of direct manipulation of data by knowledgeable programmers and circumvention of information accuracy and integrity controls.

4. **We recommend that the Automation Policy and Programs Committee (APPC) promulgate change control guidelines for distributed systems and promote the need for change control among the Board's divisions and offices.**

We interviewed management and staff from IRM and four distributed processing groups in other divisions and found no standard change control policies and procedures in effect. Division staff agreed with the need for Boardwide leadership in advocating and preparing guidelines for distributed systems. One expressed concern that these guidelines not be strict standards that rigidly confine their diverse distributed processing needs. Three interviewed also indicated that they would rather have guidelines developed by a group familiar with distributed environments rather than IRM. IRM, likewise, agrees that such guidance is needed and believes that users need to “buy into” a change control process rather than have one dictated by IRM. We believe that the APPC is in the best position to have this guidance developed and promulgated for the Board's distributed systems.

ANALYSIS OF COMMENTS

In considering our recommendations, the Director of IRM partially concurred with two recommendations and disagreed with two. Specifically, the director does not believe that a more comprehensive change control process is justified (recommendation 1), but plans to reiterate the importance of change control and explain the interrelationship of Federal Reserve System procedures and IRM's change control form during staff briefings on the new version of the Federal Reserve System's *Information Security Manual*. The director agreed to ensure that the Panvalet library management software is used consistently throughout the division (recommendation 2) but does not agree that a single library package should be used. Further, he does not agree that programmer access to application software should be more restricted. Instead, he agreed to review programmer access privileges to mainframe-based systems on an annual basis. He also does not believe that programmers’ access to production data should be further restricted (recommendation 3). Regarding our recommendation that the APPC promulgate change control guidelines for the distributed processing environment (recommendation 4), the director indicates that the Distributed Processing Advisory Group to the APPC agreed that such procedures are warranted, but only in circumstances where there is a reasonable degree of risk.

Overall, we believe the director's response illustrates a fundamental disagreement with our view regarding the level of internal controls needed for the Board's automation environment. Except in cases when data are very sensitive or represent financial value, IRM officials and staff believe the cost of more stringent change control procedures and more restrictive access to production data and applications outweigh the benefits. We continue to believe additional controls are needed to ensure the integrity of the Board's computing environment. Our recommendations are congruent with standard industry practices, including those of the Reserve Banks, and we do not believe there are major cost implications associated with implementing our suggested changes. Furthermore, IRM programmers should not need consistent access to the Board's production applications and data. The Board’s application software development process should meet user requirements and produce quality data without frequent programmer intervention.